adoption by the Federal Government, and encourage the appropriate adoption by other agencies and organizations, of the recommendations of the Team with respect to—

(A) technical aspects of evacuation and emergency response procedures;

(B) specific improvements to building standards, codes, and practices; and

(C) other actions needed to help prevent future building failures.

(Pub. L. 107–231, §9, Oct. 1, 2002, 116 Stat. 1475.)

§ 7309. National Institute of Standards and Technology annual report

Not later than February 15 of each year, the Director shall transmit to the Committee on Science of the House of Representatives and to the Committee on Commerce, Science, and Transportation of the Senate a report that includes—

(1) a summary of the investigations conducted by Teams during the prior fiscal year;

(2) a summary of recommendations made by the Teams in reports issued under section 7307 of this title during the prior fiscal year and a description of the extent to which those recommendations have been implemented; and

(3) a description of the actions taken to improve building safety and structural integrity by the National Institute of Standards and Technology during the prior fiscal year in response to reports issued under section 7307 of this title.

(Pub. L. 107–231, §10, Oct. 1, 2002, 116 Stat. 1476.)

CHANGE OF NAME

Committee on Science of House of Representatives changed to Committee on Science and Technology of House of Representatives by House Resolution No. 6, One Hundred Tenth Congress, Jan. 5, 2007.

§ 7310. Advisory committee

(a) Establishment and functions

The Director, in consultation with the United States Fire Administration and other appropriate Federal agencies, shall establish an advisory committee to advise the Director on carrying out this chapter and to review the procedures developed under section 7301(c)(1) of this title and the reports issued under section 7307 of this title.

(b) Annual report

On January 1 of each year, the advisory committee shall transmit to the Committee on Science of the House of Representatives and to the Committee on Commerce, Science, and Transportation of the Senate a report that includes—

(1) an evaluation of Team activities, along with recommendations to improve the operation and effectiveness of Teams; and

(2) an assessment of the implementation of the recommendations of Teams and of the advisory committee.

(c) Duration of advisory committee

Section 14 of the Federal Advisory Committee Act shall not apply to the advisory committee established under this section.

(Pub. L. 107–231, §11, Oct. 1, 2002, 116 Stat. 1476.)

REFERENCES IN TEXT

Section 14 of the Federal Advisory Committee Act, referred to in subsec. (c), is section 14 of Pub. L. 92–463, which is set out in the Appendix to Title 5, Government Organization and Employees.

CHANGE OF NAME

Committee on Science of House of Representatives changed to Committee on Science and Technology of House of Representatives by House Resolution No. 6, One Hundred Tenth Congress, Jan. 5, 2007.

§ 7311. Additional applicability

The authorities and restrictions applicable under this chapter to the Director and to Teams shall apply to the activities of the National Institute of Standards and Technology in response to the attacks of September 11, 2001.

(Pub. L. 107–231, §12, Oct. 1, 2002, 116 Stat. 1476.)

§ 7312. Construction

Nothing in this chapter shall be construed to confer any authority on the National Institute of Standards and Technology to require the adoption of building standards, codes, or practices.

(Pub. L. 107–231, §14, Oct. 1, 2002, 116 Stat. 1477.)

§ 7313. Authorization of appropriations

The National Institute of Standards and Technology is authorized to use funds otherwise authorized by law to carry out this chapter.

(Pub. L. 107–231, §15, Oct. 1, 2002, 116 Stat. 1477.)

CHAPTER 100—CYBER SECURITY RESEARCH AND DEVELOPMENT

§ 7401. Findings

The Congress finds the following:

(1) Revolutionary advancements in computing and communications technology have interconnected government, commercial, scientific, and educational infrastructures—including critical infrastructures for electric power, natural gas and petroleum production and distribution, telecommunications, transportation, water supply, banking and finance, and emergency and government services—in a vast, interdependent physical and electronic network.

(2) Exponential increases in interconnectivity have facilitated enhanced com-

munications, economic growth, and the delivery of services critical to the public welfare, but have also increased the consequences of temporary or prolonged failure.

(3) A Department of Defense Joint Task Force concluded after a 1997 United States information warfare exercise that the results ''clearly demonstrated our lack of preparation for a coordinated cyber and physical attack on our critical military and civilian infrastructure''.

(4) Computer security technology and systems implementation lack—

(A) sufficient long term research funding;

(B) adequate coordination across Federal and State government agencies and among government, academia, and industry; and

(C) sufficient numbers of outstanding researchers in the field.

(5) Accordingly, Federal investment in computer and network security research and development must be significantly increased to—

(A) improve vulnerability assessment and technological and systems solutions;

(B) expand and improve the pool of information security professionals, including researchers, in the United States workforce; and

(C) better coordinate information sharing and collaboration among industry, government, and academic research projects.

(6) While African-Americans, Hispanics, and Native Americans constitute 25 percent of the total United States workforce and 30 percent of the college-age population, members of these minorities comprise less than 7 percent of the United States computer and information science workforce.

(Pub. L. 107–305, § 2, Nov. 27, 2002, 116 Stat. 2367.)

SHORT TITLE

Pub. L. 107–305, § 1, Nov. 27, 2002, 116 Stat. 2367, provided that: ''This Act [enacting this chapter and section 278h of this title, amending sections 278g–3, 1511e, and 7301 of this title and section 1862 of Title 42, The Public Health and Welfare, and redesignating section 278h of this title as 278q of this title] may be cited as the 'Cyber Security Research and Development Act'.''

§ 7402. Definitions

In this chapter:

(1) Director

The term ''Director'' means the Director of the National Science Foundation.

(2) Institution of higher education

The term ''institution of higher education'' has the meaning given that term in section 1001(a) of title 20.

(Pub. L. 107–305, § 3, Nov. 27, 2002, 116 Stat. 2368.)

REFERENCES IN TEXT

This chapter, referred to in text, was in the original ''this Act'', meaning Pub. L. 107–305, Nov. 27, 2002, 116 Stat. 2367, which is classified principally to this chapter. For complete classification of this Act to the Code, see Short Title note set out under section 7401 of this title and Tables.

§ 7403. National Science Foundation research

(a) Computer and network security research grants

(1) In general

The Director shall award grants for basic research on innovative approaches to the structure of computer and network hardware and software that are aimed at enhancing computer security. Research areas may include—

(A) authentication, cryptography, and other secure data communications technology;

(B) computer forensics and intrusion detection;

(C) reliability of computer and network applications, middleware, operating systems, control systems, and communications infrastructure;

(D) privacy and confidentiality;

(E) network security architecture, including tools for security administration and analysis;

(F) emerging threats;

(G) vulnerability assessments and techniques for quantifying risk;

(H) remote access and wireless security; and

(I) enhancement of law enforcement ability to detect, investigate, and prosecute cyber-crimes, including those that involve piracy of intellectual property.

(2) Merit review; competition

Grants shall be awarded under this section on a merit-reviewed competitive basis.

(3) Authorization of appropriations

There are authorized to be appropriated to the National Science Foundation to carry out this subsection—

(A) $35,000,000 for fiscal year 2003;

(B) $40,000,000 for fiscal year 2004;

(C) $46,000,000 for fiscal year 2005;

(D) $52,000,000 for fiscal year 2006; and

(E) $60,000,000 for fiscal year 2007.

(b) Computer and network security research centers

(1) In general

The Director shall award multiyear grants, subject to the availability of appropriations, to institutions of higher education, nonprofit research institutions, or consortia thereof to establish multidisciplinary Centers for Computer and Network Security Research. Institutions of higher education, nonprofit research institutions, or consortia thereof receiving such grants may partner with 1 or more government laboratories or for-profit institutions, or other institutions of higher education or nonprofit research institutions.

(2) Merit review; competition

Grants shall be awarded under this subsection on a merit-reviewed competitive basis.

(3) Purpose

The purpose of the Centers shall be to generate innovative approaches to computer and network security by conducting cutting-edge, multidisciplinary research in computer and

network security, including the research areas described in subsection (a)(1) of this section.

(4) Applications

An institution of higher education, nonprofit research institution, or consortia thereof seeking funding under this subsection shall submit an application to the Director at such time, in such manner, and containing such information as the Director may require. The application shall include, at a minimum, a description of—

(A) the research projects that will be undertaken by the Center and the contributions of each of the participating entities;

(B) how the Center will promote active collaboration among scientists and engineers from different disciplines, such as computer scientists, engineers, mathematicians, and social science researchers;

(C) how the Center will contribute to increasing the number and quality of computer and network security researchers and other professionals, including individuals from groups historically underrepresented in these fields; and

(D) how the center[1] will disseminate research results quickly and widely to improve cyber security in information technology networks, products, and services.

(5) Criteria

In evaluating the applications submitted under paragraph (4), the Director shall consider, at a minimum—

(A) the ability of the applicant to generate innovative approaches to computer and network security and effectively carry out the research program;

(B) the experience of the applicant in conducting research on computer and network security and the capacity of the applicant to foster new multidisciplinary collaborations;

(C) the capacity of the applicant to attract and provide adequate support for a diverse group of undergraduate and graduate students and postdoctoral fellows to pursue computer and network security research; and

(D) the extent to which the applicant will partner with government laboratories, for-profit entities, other institutions of higher education, or nonprofit research institutions, and the role the partners will play in the research undertaken by the Center.

(6) Annual meeting

The Director shall convene an annual meeting of the Centers in order to foster collaboration and communication between Center participants.

(7) Authorization of appropriations

There are authorized to be appropriated for the National Science Foundation to carry out this subsection—

(A) $12,000,000 for fiscal year 2003;

(B) $24,000,000 for fiscal year 2004;

(C) $36,000,000 for fiscal year 2005;

(D) $36,000,000 for fiscal year 2006; and

(E) $36,000,000 for fiscal year 2007.

(Pub. L. 107–305, § 4, Nov. 27, 2002, 116 Stat. 2368.)

[1] So in original. Probably should be capitalized.

§ 7404. National Science Foundation computer and network security programs

(a) Computer and network security capacity building grants

(1) In general

The Director shall establish a program to award grants to institutions of higher education (or consortia thereof) to establish or improve undergraduate and master's degree programs in computer and network security, to increase the number of students, including the number of students from groups historically underrepresented in these fields, who pursue undergraduate or master's degrees in fields related to computer and network security, and to provide students with experience in government or industry related to their computer and network security studies.

(2) Merit review

Grants shall be awarded under this subsection on a merit-reviewed competitive basis.

(3) Use of funds

Grants awarded under this subsection shall be used for activities that enhance the ability of an institution of higher education (or consortium thereof) to provide high-quality undergraduate and master's degree programs in computer and network security and to recruit and retain increased numbers of students to such programs. Activities may include—

(A) revising curriculum to better prepare undergraduate and master's degree students for careers in computer and network security;

(B) establishing degree and certificate programs in computer and network security;

(C) creating opportunities for undergraduate students to participate in computer and network security research projects;

(D) acquiring equipment necessary for student instruction in computer and network security, including the installation of testbed networks for student use;

(E) providing opportunities for faculty to work with local or Federal Government agencies, private industry, nonprofit research institutions, or other academic institutions to develop new expertise or to formulate new research directions in computer and network security;

(F) establishing collaborations with other academic institutions or academic departments that seek to establish, expand, or enhance programs in computer and network security;

(G) establishing student internships in computer and network security at government agencies or in private industry;

(H) establishing collaborations with other academic institutions to establish or enhance a web-based collection of computer and network security courseware and laboratory exercises for sharing with other institutions of higher education, including community colleges;

(I) establishing or enhancing bridge programs in computer and network security between community colleges and universities; and

(J) any other activities the Director determines will accomplish the goals of this subsection.

(4) Selection process

(A) Application

An institution of higher education (or a consortium thereof) seeking funding under this subsection shall submit an application to the Director at such time, in such manner, and containing such information as the Director may require. The application shall include, at a minimum—

(i) a description of the applicant's computer and network security research and instructional capacity, and in the case of an application from a consortium of institutions of higher education, a description of the role that each member will play in implementing the proposal;

(ii) a comprehensive plan by which the institution or consortium will build instructional capacity in computer and information security;

(iii) a description of relevant collaborations with government agencies or private industry that inform the instructional program in computer and network security;

(iv) a survey of the applicant's historic student enrollment and placement data in fields related to computer and network security and a study of potential enrollment and placement for students enrolled in the proposed computer and network security program; and

(v) a plan to evaluate the success of the proposed computer and network security program, including post-graduation assessment of graduate school and job placement and retention rates as well as the relevance of the instructional program to graduate study and to the workplace.

(B) Awards

(i) The Director shall ensure, to the extent practicable, that grants are awarded under this subsection in a wide range of geographic areas and categories of institutions of higher education, including minority serving institutions.

(ii) The Director shall award grants under this subsection for a period not to exceed 5 years.

(5) Assessment required

The Director shall evaluate the program established under this subsection no later than 6 years after the establishment of the program. At a minimum, the Director shall evaluate the extent to which the program achieved its objectives of increasing the quality and quantity of students, including students from groups historically underrepresented in computer and network security related disciplines, pursuing undergraduate or master's degrees in computer and network security.

(6) Authorization of appropriations

There are authorized to be appropriated to the National Science Foundation to carry out this subsection—

(A) $15,000,000 for fiscal year 2003;
(B) $20,000,000 for fiscal year 2004;
(C) $20,000,000 for fiscal year 2005;
(D) $20,000,000 for fiscal year 2006; and
(E) $20,000,000 for fiscal year 2007.

(b) Scientific and Advanced Technology Act of 1992

(1) Grants

The Director shall provide grants under the Scientific and Advanced Technology Act of 1992 (42 U.S.C. 1862i) [42 U.S.C. 1862h et seq.] for the purposes of section 3(a) and (b) of that Act [42 U.S.C. 1862i(a), (b)], except that the activities supported pursuant to this subsection shall be limited to improving education in fields related to computer and network security.

(2) Authorization of appropriations

There are authorized to be appropriated to the National Science Foundation to carry out this subsection—

(A) $1,000,000 for fiscal year 2003;
(B) $1,250,000 for fiscal year 2004;
(C) $1,250,000 for fiscal year 2005;
(D) $1,250,000 for fiscal year 2006; and
(E) $1,250,000 for fiscal year 2007.

(c) Graduate traineeships in computer and network security research

(1) In general

The Director shall establish a program to award grants to institutions of higher education to establish traineeship programs for graduate students who pursue computer and network security research leading to a doctorate degree by providing funding and other assistance, and by providing graduate students with research experience in government or industry related to the students' computer and network security studies.

(2) Merit review

Grants shall be provided under this subsection on a merit-reviewed competitive basis.

(3) Use of funds

An institution of higher education shall use grant funds for the purposes of—

(A) providing traineeships to students who are citizens, nationals, or lawfully admitted permanent resident aliens of the United States and are pursuing research in computer or network security leading to a doctorate degree;

(B) paying tuition and fees for students receiving traineeships under subparagraph (A);

(C) establishing scientific internship programs for students receiving traineeships under subparagraph (A) in computer and network security at for-profit institutions, nonprofit research institutions, or government laboratories; and

(D) other costs associated with the administration of the program.

(4) Traineeship amount

Traineeships provided under paragraph (3)(A) shall be in the amount of $25,000 per

year, or the level of the National Science Foundation Graduate Research Fellowships, whichever is greater, for up to 3 years.

(5) Selection process

An institution of higher education seeking funding under this subsection shall submit an application to the Director at such time, in such manner, and containing such information as the Director may require. The application shall include, at a minimum, a description of—

(A) the instructional program and research opportunities in computer and network security available to graduate students at the applicant's institution; and

(B) the internship program to be established, including the opportunities that will be made available to students for internships at for-profit institutions, nonprofit research institutions, and government laboratories.

(6) Review of applications

In evaluating the applications submitted under paragraph (5), the Director shall consider—

(A) the ability of the applicant to effectively carry out the proposed program;

(B) the quality of the applicant's existing research and education programs;

(C) the likelihood that the program will recruit increased numbers of students, including students from groups historically underrepresented in computer and network security related disciplines, to pursue and earn doctorate degrees in computer and network security;

(D) the nature and quality of the internship program established through collaborations with government laboratories, nonprofit research institutions, and for-profit institutions;

(E) the integration of internship opportunities into graduate students' research; and

(F) the relevance of the proposed program to current and future computer and network security needs.

(7) Authorization of appropriations

There are authorized to be appropriated to the National Science Foundation to carry out this subsection—

(A) $10,000,000 for fiscal year 2003;

(B) $20,000,000 for fiscal year 2004;

(C) $20,000,000 for fiscal year 2005;

(D) $20,000,000 for fiscal year 2006; and

(E) $20,000,000 for fiscal year 2007.

(d) Graduate Research Fellowships program support

Computer and network security shall be included among the fields of specialization supported by the National Science Foundation's Graduate Research Fellowships program under section 1869 of title 42.

(e) Cyber security faculty development traineeship program

(1) In general

The Director shall establish a program to award grants to institutions of higher education to establish traineeship programs to enable graduate students to pursue academic careers in cyber security upon completion of doctoral degrees.

(2) Merit review; competition

Grants shall be awarded under this section on a merit-reviewed competitive basis.

(3) Application

Each institution of higher education desiring to receive a grant under this subsection shall submit an application to the Director at such time, in such manner, and containing such information as the Director shall require.

(4) Use of funds

Funds received by an institution of higher education under this paragraph shall—

(A) be made available to individuals on a merit-reviewed competitive basis and in accordance with the requirements established in paragraph (7);

(B) be in an amount that is sufficient to cover annual tuition and fees for doctoral study at an institution of higher education for the duration of the graduate traineeship, and shall include, in addition, an annual living stipend of $25,000; and

(C) be provided to individuals for a duration of no more than 5 years, the specific duration of each graduate traineeship to be determined by the institution of higher education, on a case-by-case basis.

(5) Repayment

Each graduate traineeship shall—

(A) subject to paragraph (5)(B), be subject to full repayment upon completion of the doctoral degree according to a repayment schedule established and administered by the institution of higher education;

(B) be forgiven at the rate of 20 percent of the total amount of the graduate traineeship assistance received under this section for each academic year that a recipient is employed as a full-time faculty member at an institution of higher education for a period not to exceed 5 years; and

(C) be monitored by the institution of higher education receiving a grant under this subsection to ensure compliance with this subsection.

(6) Exceptions

The Director may provide for the partial or total waiver or suspension of any service obligation or payment by an individual under this section whenever compliance by the individual is impossible or would involve extreme hardship to the individual, or if enforcement of such obligation with respect to the individual would be unconscionable.

(7) Eligibility

To be eligible to receive a graduate traineeship under this section, an individual shall—

(A) be a citizen, national, or lawfully admitted permanent resident alien of the United States; and

(B) demonstrate a commitment to a career in higher education.

(8) Consideration

In making selections for graduate traineeships under this paragraph, an institution re-

ceiving a grant under this subsection shall consider, to the extent possible, a diverse pool of applicants whose interests are of an interdisciplinary nature, encompassing the social scientific as well as the technical dimensions of cyber security.

(9) Authorization of appropriations

There are authorized to be appropriated to the National Science Foundation to carry out this paragraph $5,000,000 for each of fiscal years 2003 through 2007.

(Pub. L. 107–305, § 5, Nov. 27, 2002, 116 Stat. 2370.)

REFERENCES IN TEXT

The Scientific and Advanced Technology Act of 1992, referred to in subsec. (b)(1), is Pub. L. 102–476, Oct. 23, 1992, 106 Stat. 2297, as amended, which is classified generally to section 1862h et seq. of Title 42, The Public Health and Welfare. For complete classification of this Act to the Code, see Short Title note set out under section 1861 of Title 42 and Tables.

§ 7405. Consultation

In carrying out sections 7403 and 7404 of this title, the Director shall consult with other Federal agencies.

(Pub. L. 107–305, § 6, Nov. 27, 2002, 116 Stat. 2374.)

§ 7406. National Institute of Standards and Technology programs

(a), (b) Omitted

(c) Checklists for Government systems

(1) In general

The Director of the National Institute of Standards and Technology shall develop, and revise as necessary, a checklist setting forth settings and option selections that minimize the security risks associated with each computer hardware or software system that is, or is likely to become, widely used within the Federal Government.

(2) Priorities for development; excluded systems

The Director of the National Institute of Standards and Technology may establish priorities for the development of checklists under this paragraph on the basis of the security risks associated with the use of the system, the number of agencies that use a particular system, the usefulness of the checklist to Federal agencies that are users or potential users of the system, or such other factors as the Director determines to be appropriate. The Director of the National Institute of Standards and Technology may exclude from the application of paragraph (1) any computer hardware or software system for which the Director of the National Institute of Standards and Technology determines that the development of a checklist is inappropriate because of the infrequency of use of the system, the obsolescence of the system, or the inutility or impracticability of developing a checklist for the system.

(3) Dissemination of checklists

The Director of the National Institute of Standards and Technology shall make any checklist developed under this paragraph for any computer hardware or software system available to each Federal agency that is a user or potential user of the system.

(4) Agency use requirements

The development of a checklist under paragraph (1) for a computer hardware or software system does not—

(A) require any Federal agency to select the specific settings or options recommended by the checklist for the system;

(B) establish conditions or prerequisites for Federal agency procurement or deployment of any such system;

(C) represent an endorsement of any such system by the Director of the National Institute of Standards and Technology; nor

(D) preclude any Federal agency from procuring or deploying other computer hardware or software systems for which no such checklist has been developed.

(d) Federal agency information security programs

(1) In general

In developing the agencywide information security program required by section 3534(b) of title 44, an agency that deploys a computer hardware or software system for which the Director of the National Institute of Standards and Technology has developed a checklist under subsection (c) of this section—

(A) shall include in that program an explanation of how the agency has considered such checklist in deploying that system; and

(B) may treat the explanation as if it were a portion of the agency's annual performance plan properly classified under criteria established by an Executive Order (within the meaning of section 1115(d) of title 31).

(2) Limitation

Paragraph (1) does not apply to any computer hardware or software system for which the National Institute of Standards and Technology does not have responsibility under section 278g–3(a)(3) of this title.

(Pub. L. 107–305, § 8, Nov. 27, 2002, 116 Stat. 2375.)

CODIFICATION

Section is comprised of section 8 of Pub. L. 107–305. Subsec. (a) of section 8 of Pub. L. 107–305 enacted section 278h of this title and renumbered former section 278h of this title as section 278q of this title. Subsec. (b) of section 8 of Pub. L. 107–305 amended section 278g–3 of this title.

§ 7407. Authorization of appropriations

There are authorized to be appropriated to the Secretary of Commerce for the National Institute of Standards and Technology—

(1) for activities under section 278h of this title—

(A) $25,000,000 for fiscal year 2003;

(B) $40,000,000 for fiscal year 2004;

(C) $55,000,000 for fiscal year 2005;

(D) $70,000,000 for fiscal year 2006;

(E) $85,000,000 for fiscal year 2007; and

(2) for activities under section 278g–3(f) of this title—

(A) $6,000,000 for fiscal year 2003;
(B) $6,200,000 for fiscal year 2004;
(C) $6,400,000 for fiscal year 2005;
(D) $6,600,000 for fiscal year 2006; and
(E) $6,800,000 for fiscal year 2007.

(Pub. L. 107–305, § 11, Nov. 27, 2002, 116 Stat. 2379.)

§ 7408. National Academy of Sciences study on computer and network security in critical infrastructures

(a) Study

Not later than 3 months after November 27, 2002, the Director of the National Institute of Standards and Technology shall enter into an arrangement with the National Research Council of the National Academy of Sciences to conduct a study of the vulnerabilities of the Nation's network infrastructure and make recommendations for appropriate improvements. The National Research Council shall—

(1) review existing studies and associated data on the architectural, hardware, and software vulnerabilities and interdependencies in United States critical infrastructure networks;

(2) identify and assess gaps in technical capability for robust critical infrastructure network security and make recommendations for research priorities and resource requirements; and

(3) review any and all other essential elements of computer and network security, including security of industrial process controls, to be determined in the conduct of the study.

(b) Report

The Director of the National Institute of Standards and Technology shall transmit a report containing the results of the study and recommendations required by subsection (a) of this section to the Senate Committee on Commerce, Science, and Transportation and the House of Representatives Committee on Science not later than 21 months after November 27, 2002.

(c) Security

The Director of the National Institute of Standards and Technology shall ensure that no information that is classified is included in any publicly released version of the report required by this section.

(d) Authorization of appropriations

There are authorized to be appropriated to the Secretary of Commerce for the National Institute of Standards and Technology for the purposes of carrying out this section, $700,000.

(Pub. L. 107–305, § 12, Nov. 27, 2002, 116 Stat. 2380.)

CHANGE OF NAME

Committee on Science of House of Representatives changed to Committee on Science and Technology of House of Representatives by House Resolution No. 6, One Hundred Tenth Congress, Jan. 5, 2007.

§ 7409. Coordination of Federal cyber security research and development

The Director of the National Science Foundation and the Director of the National Institute of Standards and Technology shall coordinate the research programs authorized by this chapter or pursuant to amendments made by this chapter. The Director of the Office of Science and Technology Policy shall work with the Director of the National Science Foundation and the Director of the National Institute of Standards and Technology to ensure that programs authorized by this chapter or pursuant to amendments made by this chapter are taken into account in any government-wide cyber security research effort.

(Pub. L. 107–305, § 13, Nov. 27, 2002, 116 Stat. 2380.)

REFERENCES IN TEXT

This chapter, referred to in text, was in the original ''this Act'', meaning Pub. L. 107–305, Nov. 27, 2002, 116 Stat. 2367, which is classified principally to this chapter. For complete classification of this Act to the Code, see Short Title note set out under section 7401 of this title.

§ 7410. Grant eligibility requirements and compliance with immigration laws

(a) Immigration status

No grant or fellowship may be awarded under this chapter, directly or indirectly, to any individual who is in violation of the terms of his or her status as a nonimmigrant under section 1101(a)(15)(F), (M), or (J) of title 8.

(b) Aliens from certain countries

No grant or fellowship may be awarded under this chapter, directly or indirectly, to any alien from a country that is a state sponsor of international terrorism, as defined under section 1735(b) of title 8, unless the Secretary of State determines, in consultation with the Attorney General and the heads of other appropriate agencies, that such alien does not pose a threat to the safety or national security of the United States.

(c) Non-complying institutions

No grant or fellowship may be awarded under this chapter, directly or indirectly, to any institution of higher education or non-profit institution (or consortia thereof) that has—

(1) materially failed to comply with the recordkeeping and reporting requirements to receive nonimmigrant students or exchange visitor program participants under section 1101(a)(15)(F), (M), or (J) of title 8, or section 1372 of title 8, as required by section 1762 of title 8; or

(2) been suspended or terminated pursuant to section 1762(c) of title 8.

(Pub. L. 107–305, § 16, Nov. 27, 2002, 116 Stat. 2381.)

§ 7411. Report on grant and fellowship programs

Within 24 months after November 27, 2002, the Director, in consultation with the Assistant to the President for National Security Affairs, shall submit to Congress a report reviewing this chapter to ensure that the programs and fellowships are being awarded under this chapter to individuals and institutions of higher education who are in compliance with the Immigration and Nationality Act (8 U.S.C. 1101 et seq.) in order to protect our national security.

(Pub. L. 107–305, § 17, Nov. 27, 2002, 116 Stat. 2381.)

REFERENCES IN TEXT

The Immigration and Nationality Act, referred to in text, is act June 27, 1952, ch. 477, 66 Stat. 163, as amend-

ed, which is classified principally to chapter 12 (§ 1101 et seq.) of Title 8, Aliens and Nationality. For complete classification of this Act to the Code, see Short Title note set out under section 1101 of Title 8 and Tables.

CHAPTER 101—NANOTECHNOLOGY RESEARCH AND DEVELOPMENT

§ 7501. National Nanotechnology Program

(a) National Nanotechnology Program

The President shall implement a National Nanotechnology Program. Through appropriate agencies, councils, and the National Nanotechnology Coordination Office established in section 7502 of this title, the Program shall—

(1) establish the goals, priorities, and metrics for evaluation for Federal nanotechnology research, development, and other activities;

(2) invest in Federal research and development programs in nanotechnology and related sciences to achieve those goals; and

(3) provide for interagency coordination of Federal nanotechnology research, development, and other activities undertaken pursuant to the Program.

(b) Program activities

The activities of the Program shall include—

(1) developing a fundamental understanding of matter that enables control and manipulation at the nanoscale;

(2) providing grants to individual investigators and interdisciplinary teams of investigators;

(3) establishing a network of advanced technology user facilities and centers;

(4) establishing, on a merit-reviewed and competitive basis, interdisciplinary nanotechnology research centers, which shall—

(A) interact and collaborate to foster the exchange of technical information and best practices;

(B) involve academic institutions or national laboratories and other partners, which may include States and industry;

(C) make use of existing expertise in nanotechnology in their regions and nationally;

(D) make use of ongoing research and development at the micrometer scale to support their work in nanotechnology; and

(E) to the greatest extent possible, be established in geographically diverse locations, encourage the participation of Historically Black Colleges and Universities that are part B institutions as defined in section 1061(2) of title 20 and minority institutions (as defined in section 1067k(3) of title 20), and include institutions located in States participating in the Experimental Program to Stimulate Competitive Research (EPSCoR);

(5) ensuring United States global leadership in the development and application of nanotechnology;

(6) advancing the United States productivity and industrial competitiveness through stable, consistent, and coordinated investments in long-term scientific and engineering research in nanotechnology;

(7) accelerating the deployment and application of nanotechnology research and development in the private sector, including startup companies;

(8) encouraging interdisciplinary research, and ensuring that processes for solicitation and evaluation of proposals under the Program encourage interdisciplinary projects and collaborations;

(9) providing effective education and training for researchers and professionals skilled in the interdisciplinary perspectives necessary for nanotechnology so that a true interdisciplinary research culture for nanoscale science, engineering, and technology can emerge;

(10) ensuring that ethical, legal, environmental, and other appropriate societal concerns, including the potential use of nanotechnology in enhancing human intelligence and in developing artificial intelligence which exceeds human capacity, are considered during the development of nanotechnology by—

(A) establishing a research program to identify ethical, legal, environmental, and other appropriate societal concerns related to nanotechnology, and ensuring that the results of such research are widely disseminated;

(B) requiring that interdisciplinary nanotechnology research centers established under paragraph (4) include activities that address societal, ethical, and environmental concerns;

(C) insofar as possible, integrating research on societal, ethical, and environmental concerns with nanotechnology research and development, and ensuring that advances in nanotechnology bring about improvements in quality of life for all Americans; and

(D) providing, through the National Nanotechnology Coordination Office established in section 7502 of this title, for public input and outreach to be integrated into the Program by the convening of regular and ongoing public discussions, through mechanisms such as citizens' panels, consensus conferences, and educational events, as appropriate; and

(11) encouraging research on nanotechnology advances that utilize existing processes and technologies.

(c) Program management

The National Science and Technology Council shall oversee the planning, management, and coordination of the Program. The Council, itself or